LAP (Local Association Protocol) Specification

Overview

This Local Access Pairing Specification documents the steps and messages that are used to pair and communicate with Lutron systems that support local network control.

General LAP Requirements

1. Connection to LAP Server uses Client Authentication with TLS v1.2
2. Certificates are in the x.509 format and sent in request/responses in the PEM format (https://en.wikipedia.org/wiki/Privacy-enhanced_Electronic_Mail)
3. All messages from the client to the server must be \n terminated.
4. All messages from the server to the client will be \r\n terminated.
5. The ClientTag of a request will be echoed in the corresponding response.
6. The ClientTag may be any legal JSON type (string, object, etc.).
7. The ClientTag of a subscribe request will also be echoed in every corresponding notification.
8. If the server does not receive a message from the client for 5 minutes, the server will terminate the connection. Use the Ping request as a keep alive if the session must stay alive.
9. All requests require Public permission unless otherwise specified.
10. PhysicalAccess permission is granted if the client is connected before the button on the Bridge is pressed.
11. If the client does not have the necessary permissions to perform a request or a message is not malformed or not acceptable, an exception is received.

Commands:

Ping Request

Client sends ping request

```
{
  "Header": {
    "RequestType": "Ping",
    "ClientTag": "..."
  }
}
```

Bridge sends response and resets connection timeout to 5 minutes.

```
{
  "Header": {
    "StatusCode": "204 No Content",
    "ClientTag": "..."
  }
}
```

Asynchronous Notification of Elevated Privileges when Button is Pressed

Bridge sends notification

```
{
  "Header": {
    "StatusCode": "200 OK",
    "ContentType": "status;plurality=single"
  },
  "Body": {
    "Status": {
      "Permissions": [
        "Public",
        "PhysicalAccess"
      ]
    }
  }
}
```

Client Sends CSR to set up Pairing (requires PhysicalAccess permission)

- Bridge will verify contents of CSR are acceptable for the client device and will respond with an exception if they are not acceptable.

Client sends execute request

```
{
   "Header":{
      "RequestType":"Execute",
      "ClientTag":"...",
      "Url":"/pair"
   },
   "Body":{
      "CommandType":"CSR",
      "Parameters":{
         "CSR":"...",
         "DisplayName":"...", // User Friendly name of Client Device
         "DeviceUID":"..."    // Unique ID of Client Device
      }
   }
}
```

Bridge sends response if permission has been granted

```
{
   "Header":{
      "StatusCode":"200 OK",
      "ClientTag":"...",
      "ContentType":"signing-result;plurality=single"
   },
   "Body":{
      "SigningResult":{
         "Certificate":"...",   // The certificate issued to the client
         "RootCertificate":"..."  // The root certificate that the issued certificate chains to
      }
   }
}
```

Bridge sends response if permission not allowed

```
{
   "Header":{
      "StatusCode":"401 Unauthorized",
      "ClientTag":"…",
      "ContentType":"exception;plurality=single"
   },
   "Body":{
      "Exception":{
         "Message":"You are not authorized to perform this request"
      }
   }
}
```

Client Reads Root Certificate of LAP Server

Client sends read request

```
{
   "Header":{
      "RequestType":"Read",
      "ClientTag":"...",
      "Url":"/certificate/root"
   }
}
```

Bridge sends response

```
{
   "Header":{
      "StatusCode":"200 OK",
      "ClientTag":"...",
      "ContentType":"certificate;plurality=single"
   },
   "Body":{
      "Certificate":{
         "href":"/certificate/root",
         "Certificate":"..."
      }
   }
}
```

Client Reads MAC Address of Lutron Bridge

Client sends read request

```
{
   "Header":{
      "RequestType":"Read",
      "ClientTag":"...",
      "Url":"/system/macaddress"
   }
}
```

Bridge sends response

```
{
   "Header":{
      "StatusCode":"200 OK",
      "ClientTag":"...",
      "ContentType":"macaddress;plurality=single"
   },
   "Body":{
      "MACAddress":{
         "href":"/system/macaddress",
         "MACAddress":"123456789ABC"
      }
   }
}
```

Definitions:

Example Pairing Flows

Client Device - device that is going to pair with the Lutron system.

Client LAP Certificate - certificate signed by Lutron that grants you permission to pair with Lutron systems; provided ahead of time by Lutron

LAP Server - server hosted by Lutron system to faciliates pairing.

LEAP Server - server hosted by the Lutron system that faciliates control of the Lutron system.

Lutron Bridge - main device of the Lutron system.

High Level Overview

Discovery

Discover the Lutron Bridge on the local network using mDNS and get the IP address of the Lutron Bridge and the ports that the LAP Server and LEAP Server are being served on.

Client Device creates a TLS connection to the LAP server

Connect to the LAP server using TLS and present the Client LAP Certificate. The LAP server requires Client Authentication at this step. (http://en.wikipedia.org/wiki/Transport_Layer_Security#Client-authenticated_TLS_handshake). You can send a ping request to verify connectivity to the LAP Server and to keep the connection alive as it will terminate after 5 minutes of inactivity. To perform Server Authentication, use the Lutron Residential Local Access Protocol CA certificate.

Prompt user to press the button on the Lutron Bridge to get pairing privilege

In order to pair, the Client Devices's connection needs to be granted elevated privileges. This is accomplished by prompting the customer to press the button on the back of the Lutron Bridge. When the customer presses the button, the LAP Server will send granted elevated permissions – physical access. At this point, the LAP server is willing to sign a certificate for the client device.

Client Device sends a Certificate Signing Request (CSR) to the Smart Bridge

After being granted privileges, generate a public/private key pair and save the pair. Using the key pair, create a Certificate Signing Request (https://en.wikipedia.org/wiki/Certificate_signing_request). Send the CSR to the LAP server. The LAP server will respond with a LEAP certificate that can be used to connect to the LEAP server. The certificate should be saved as you'll need to present it when connecting to the LEAP server. The root certificate of the same response is the certificate that issued the LEAP certificate. While the connection is still alive, request the Bridge's root certificate from the "/certificate/root" endpoint. The Bridge's root certificate should be saved to perform Server Authentication when connecting to the LEAP server later.

Connecting to LEAP Server

Connect to the LEAP server using TLS and present the certificate saved from Pairing Step 3. The LEAP server will require Client Authentication using the LEAP Certificate returned in the response to the /pair request. Perform Server Authentication using the Bridge Certificate you got back from /certificate/root. You will need to use SNI using the Common Name from the Root Certificate. Normal LEAP communication can proceed from there.

Sequence Diagram

LAP (Local Association Protocol) Specification